UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/616,805	07/14/2000	Michael P. Lyle	RECOP002	6607

21912 7590 01/27/2006

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/616,805	LYLE ET AL.	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) *1-15,18,19 and 21-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-11,14,18,19 and 21-28* is/are rejected.

7)☐ Claim(s) *12,13 and 15* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to request for reconsideration, and amendment filed on November 01, 2005. Original application contained Claims 1-24. Applicant previously amended Claims 1, 4-7, 10-17, 18, 21-24, and cancelled Claims 16, and 20. Applicant previously added new Claims 25-28. Applicant currently amended Claims 1, 23, 24, and cancelled Claim 17. The amendment filed have been entered and made of record. Presently pending claims are 1-15, 18-19, and 21-28.

Allowable Subject Matter

Claims 12, 13 and 15 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

Applicant's arguments filed on November 01, 2005 have been fully considered but they are not persuasive because of the following reasons:

Regarding independent and dependent Claims 1-6, 10-13, 15-16, and 20-24 applicants argued, *" generating fictitious content"*, and *"intentionally introducing a spelling error, grammatical error to make the deception environment appear more realistic"*, and *"relative probability of occurrence of at least one data item* ".

This is not found persuasive. The system of cited prior arts (CPA) [Bernardo et al. (U.S. Patent No. 6,247,032), Kelley (U.S. Patent No. 4,719,566)] clearly teach system and method of a software tool to use with a computer system for simplifying the creation of Web sites (such as file system). The tool comprises a plurality of pre-stored templates, comprising HTML formatting code, text, fields and formulas. The templates preferably correspond to different types of Web pages and other features commonly found on or available to Web sites. An approval module designates an approval criterion to be satisfied before the content is published on the web site. A designation module designates specified collaborators from the database of users. A schedule module sets the schedule to route the contents of created web site to specified collaborators. A building module builds the web site, based on the contents and specified features. An approval determination module determines whether approval criterion is satisfied. A posting module posts the contents of web site, based on satisfaction of approval criterion. All unauthorized access is actually connected to a false target, which continues a communication mode with the user. Because the user is bound to a false partition or interface and access paths to other partitions are blocked complete security may be preserved. Thus, by logging all messages and sending alerts and selected messages from the false interface to a security monitor, an improvement in the ability to locate those attempting system penetration is made by creating a more extensive audit trail and holding them on the line, so to speak, than would otherwise be

available. This audit trail in the false interface would be clear evidence of unauthorized access and provide a significant deterrent to unauthorized access by those aware of its installation (see Bernardo: col. 2, lines 44 to col. 3, lines 1-5, col.5 line 55 to col.6 line 20, see col. 7, lines 18-36, and Kelly: col. 1, line 66 to col.2 line 31, and col.4 line 59 to line 62).

As a result, the system of cited prior art(s) does implement and teaches a system and method for generating (fictitious) content for a computer to deceive attackers into believing they have gained access to a true computer system, without actually allowing them to gain access to true files, and to monitor such attackers, without their knowing, to facilitate efforts to improve security measures and identify attackers.

Applicants still have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that the system of cited prior arts does teach or suggest the subject matter broadly recited in independent Claims and in subsequent dependent Claims. Accordingly, rejections for claims 1-15, 18-19, and 21-28 are respectfully maintained.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-6, 10-13, 15-17, and 20-24 rejected under 35 U.S.C. 103(a) as being unpatentable over Bernardo et al. U.S. Patent No. 6,247,032 ('Bernardo' hereinafter) in view of Kelley U.S. Patent No. 4,719,566.

With respect to claim 1, Bernardo teach a method for generating computer file system content for a computing system configured to provide (see abstract; col. 2, lines 33-37), to an intruder who has gained or is attempting to gain unauthorized access to a network with which the computing system is associated, a deception environment in which the intruder is allowed to access at least part of the generated fictitious computer file system content to keep the intruder from gaining access to a protected network resources located outside the deception environment (Fig.1-2), comprising:

creating a plurality of template (see col. 2, lines 44-67 to col. 3, lines 1-5);

providing a collection of data items available to be inserted into the templates (see col. 2, lines 44-67 to col. 3, lines 1-5);

selecting one or more of said templates; and for each template selected automatically selecting at least one data item from the collection (col.5 line 55 to col.6 line 20); and

populating the template with at least one data item form the collection (see col. 3, lines 17-35);

wherein for at least one selected template, selecting the at least one data item is based at least in part on the relative probability of occurrence of the at least one data item to make the deception environment more realistic by ensuring that data items occur with the frequency one would expect in real, non-deception computing environment associated with network (see col. 7, lines 18-36).

Bernardo do not explicitly disclose generating fictitious content.

Kelley discloses generating fictitious content wherein the fictitious computer file system content is suitable for use in a deception environment in which the intruder is allowed to access at least part of the generated fictitious computer file system content to keep the intruder from gaining access to a protected network resources located outside the deception environment (see abstract; and col. 1, line 66 to col.2 line 31, and col.4 line 59 to line 62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kelley within the system of Bernardo to arrive at the invention as claimed because both references are direct to generating computer file system content, and the implementation of generating fictitious file system content would prevent an attacker seeking to gain unauthorized access to a computer or computer network by luring the would be attacker to non working files, further increasing the level of security of the network by letting only authorized users to access the network. It would have been obvious to a person of

ordinary skill in the art to extend the capability of the network by incorporating the fictitious generating content feature of Kelley to improve the security and versatility of the combined system.

3. Claim 2 rejected as above in rejecting claim 1, wherein the collection of data items comprises one or more names (see col. 7, lines 18-36).

4. Claim 3 rejected as above in rejecting claim 1, wherein the collection of data items comprises one or more dates (see col. 7, lines 18-63).

5. Claim 4 rejected as above in rejecting claim 1, wherein at least one template is an e-mail message requiring at least one item of data to be complete (see col. 7, lines 18-36).

6. Claim 5 rejected as above in rejecting claim 1, wherein at least one template is a word processing document requiring at least one item of data to be complete (see col. 1, lines 42-61).

7. Claim 6 rejected as above in rejecting claim 1, wherein at least one template is a spreadsheet requiring at least one item of data to be complete (see col. 1, lines 42-61).

8. Claim 10 rejected as above in rejecting claim 1, wherein for at least one selected template the step of populating comprises correlating a random number to an item of data in the collection (see col. 7, lines 18-36).

9. Claim 11 rejected as above in rejecting claim 1, wherein for at least one selected template the step of populating comprises inserting an item of data into the template (see col. 7, lines 18-36).

10. Claim 21 rejected as above in rejecting claim 1, further associating a probability of occurrence with each template and wherein the step of selecting comprises selecting one or more

of said templates is based at least in part on the associated probability of occurrence (see col. 7, lines 18-63).

11. Claim 22 rejected as above in rejecting claim 1, wherein at least one template requires that at least two items of data be compatible with one another (see col. 7, lines 18-63).

12. With respect to claim 23, Bernardo teach a system for generating computer file system content for a computing system configured to provide (see abstract; col. 2, lines 33-37), to an intruder who has gained or is attempting to gain unauthorized access to a network with which the computing system is associated, a deception environment in which the intruder is allowed to access at least part of the generated fictitious computer file system content to keep the intruder from gaining access to a protected network resources located outside the deception environment, comprising:

a computer configured to: (see col. 3, lines 17-35);

select one or more of a plurality of templates; and for each template selected automatically select at least one data item from a collection of data items available to be inserted into the template (col.5 line 55 to col.6 line 20); and

populate the template with at least one data item from the collection (see col. 3, lines 17-35); and

a database configured to store the collection (see col. 7, lines 18-63);

wherein for at least one selected template, selecting the at least one data item is based at least in part on the relative probability of occurrence of the at least one data item to make the deception environment more realistic by ensuring that data items occur with the frequency one would expect in real, non-deception computing environment associated with network (see col. 7, lines 18-36).

Bernardo do not explicitly disclose generating fictitious content.

Kelley discloses generating fictitious content wherein the fictitious computer file system content is suitable for use in a deception environment in which the intruder is allowed to access at least part of the generated fictitious computer file system content to keep the intruder from gaining access to a protected network resources located outside the deception environment (see abstract; and col. 1, line 66 to col.2 line 31, and col.4 line 59 to line 62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kelley within the system of Bernardo to arrive at the invention as claimed because both references are direct to generating computer file system content, and the implementation of generating fictitious file system content would prevent an attacker seeking to gain unauthorized access to a computer or computer network by luring the would be attacker to non working files, further increasing the level of security of the network by letting only authorized users to access the network. It would have been obvious to a person of ordinary skill in the art to extend the capability of the network by incorporating the fictitious generating content feature of Kelley to improve the security and versatility of the combined system.

13. With respect to claim 24, Bernardo teach a computer program product for generating file system content for a computing system configured to provide (see abstract; col. 2, lines 33-37), to an intruder who has gained or is attempting to gain unauthorized access to a network with which the computing system is associated, a deception environment in which the intruder is allowed to access at least part of the generated fictitious computer file system content to keep the intruder from gaining access to a protected network resources located outside the deception

environment, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

selecting one or more of a plurality of templates; and for each template selected: automatically selecting at least one data item from a collection of data items available to be inserted into the template (see col. 2, lines 44-67 to col. 3, lines 1-5, and col.5 line 55 to col.6 line 20); and populating the template with at least one data item from the collection (see col. 3, lines 17-35); and

a database configured to store the collection (see col. 7, lines 18-63);

wherein for at least one selected template, selecting the at least one data item is based at least in part on the relative probability of occurrence of the at least one data item to make the deception environment more realistic by ensuring that data items occur with the frequency one would expect in real, non-deception computing environment associated with network (see col. 7, lines 18-36).

Bernardo do not explicitly disclose generating fictitious content.

Kelley discloses generating fictitious content wherein the fictitious computer file system content is suitable for use in a deception environment in which the intruder is allowed to access at least part of the generated fictitious computer file system content to keep the intruder from gaining access to a protected network resources located outside the deception environment (see abstract; and col. 1, line 66 to col.2 line 31, and col.4 line 59 to line 62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kelley within the system of Bernardo to arrive at the invention as claimed because both references are direct to generating computer file system

content, and the implementation of generating fictitious file system content would prevent an attacker seeking to gain unauthorized access to a computer or computer network by luring the would be attacker to non working files, further increasing the level of security of the network by letting only authorized users to access the network. It would have been obvious to a person of ordinary skill in the art to extend the capability of the network by incorporating the fictitious generating content feature of Kelley to improve the security and versatility of the combined system.

14. Claims 25-28 are rejected applied as above rejecting claim 1. Furthermore, the system of Bernardo and Kelley teaches a system and method for generating fictitious content to deceive attackers, wherein: the collection includes at least one data item that is not fictitious (Bernardo: col.5 line 55 to col.6 line 20), the deception environment is: on a server, on a PC, and part of a trap system (Bernardo: Fig.1-2, Col2 line 28 to line 37, and Kelly: Fig.1-2, col.3 line 25 to line 65).

15. Claims 7-9, 14 and 18-19 rejected under 35 U.S.C. 103(a) as being unpatentable over Bernardo et al. U.S. Patent No. 6,247,032 ('Bernardo' hereinafter) in view of Kelley U.S. Patent No. 4,719,566, in further view of Colvin, Sr. U.S. Patent No. 6,041,123 ('Colvin' hereinafter).

17. Claim 7 rejected as above in rejecting claim 1, and Bernardo in view of Kelley teach all the limitations set forth above in claim 1.

Bernardo and Kelley do not explicitly disclose the step of populating comprises receiving a number from a random number generator.

Colvin disclose a random number generator (see col. 5, lines 22-25; col. 6, lines 60-67).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Colvin within the combined system of Bernardo and Kelley to arrive at the invention as claimed because the references are direct to generating computer file system content, and the implementation of a random number generator would enable the network system to determine the intervals at which additional file content is generated, further increasing the level of security by providing a more realistic deception environment, furthermore improving the versatility of the combined systems.

16. As to claim 8, Bernardo and Kelley do not explicitly show a pseudo random number generator. However, Colvin teaches a pseudo random number generator (see col. 5, lines 22-25; col. 6, lines 60-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Bernardo in view of Kelley in further view of Colvin for the same reasons set forth in claim 7 above.

17. As to claim 9, Bernardo and Kelley do not explicitly show a pseudo random number generator employs a unique key to generate numbers. However, Colvin teaches a pseudo random number generator employs a unique key to generate numbers (see col. 6, lines 60-67 to col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Bernardo in view of Kelley in further view of Colvin for the same reasons set forth in claim 8 above.

18. Claim 14 rejected as above in rejecting claim 13, and Bernardo and Kelley teach all the limitations set forth above as indicated in claim 13.

Bernardo and Kelley do not explicitly disclose wherein the step of populating comprises receiving a number from a random number is used to determine what the least spelling error will be.

Colvin disclose a random number (see col. 5, lines 22-25; col. 6, lines 60-67).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Colvin within the combined system of Bernardo and Kelley to arrive at the invention as claimed because the references are direct to generating computer file system content, and the implementation of a random number would enable the network system to determine the intervals at which additional file content is generated, further increasing the level of security by providing a more realistic deception environment, furthermore improving the versatility of the combined systems.

19. Claim 18 rejected as above in rejecting claim 1, and Bernardo in view of Kelley teach all the limitations set forth above in claim 1.

Bernardo and Kelly do not explicitly disclose wherein for at least one selected template, selecting the at least one data item is a function of (1) a random number and (2) the relative probability of occurrence of the at least one data item.

Colvin disclose a random number and the relative probability of occurrence of each data item (see col. 5, lines 22-25; col. 6, lines 60-67 to col. 7, lines 1-5).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Colvin within the combined system of Bernardo and Kelley to arrive at the invention as claimed because the references are direct to generating computer file system content, and the implementation of a random number generator would

enable the network system to determine the intervals at which additional file content is generated, further increasing the level of security by providing a more realistic deception environment, furthermore improving the versatility of the combined systems.

20. As to claim 19, Bernardo and Kelley do not explicitly show a pseudo random number generator provides the random number. However, Colvin teaches a pseudo random number generator employs a random number (see col. 6, lines 60-67 to col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Bernardo in view of Kelley in further view of Colvin for the same reasons set forth in claim 18 above.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

sz
January 12, 2006